Search result: 1 of 1

(WO/2003/023980) SYSTEM AND METHOD FOR SECURING A COMMUNICATION CHANNEL

Biblio. Data | Description | Claims | National Phase | Notices | Documents

Latest bibliographic data on file with the International Bureau

Pub. No.: WO/2003/023980
Publication Date: 20.03.2003
Chapter 2 Demand Filed: 10.04.2003
International Application No.: PCT/US2002/028734
International Filing Date: 10.09.2002

IPC: *H04L 9/08* (2006.01), *H04L 9/18* (2006.01)

Applicant: **WAVE7 OPTICS, INC.** [US/US]; 1075 Windward Ridge Parkway, Suite 170, Alpharetta, GA 30005 (US).

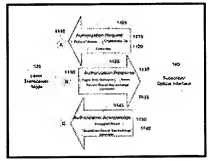
Inventors: **THOMAS, Stephen, A.**; (US).
BERSON, Thomas, A.; (US).
ANTHONY, Deven, J.; (US).
GONG, Guang; (CA).
FARMER, James, O.; (US).

Agent: **WIGMORE, Steven, P.**; King & Spalding, 191 Peachtree Street, Atlanta, GA 30303-1763 (US).

Priority Data: 60/318,447 10.09.2001 US
60/388,497 14.06.2002 US

Title: SYSTEM AND METHOD FOR SECURING A COMMUNICATION CHANNEL

Abstract: A system and method establishes a secure communication channel over an optical network (140). More specifically, the system and method can generally include securing a communications (140) channel to prevent unauthorized access such as eavesdropping or masquerading by employing 1) an encryption scheme derived from the non-linear filtering of shift registers, 2) a method for authenticating and exchanging parameters between two parties over an unsecured data channel for deriving a shared encryption key having a property of perfect forward secrecy, and 3) employing a unique format of the messages that can transport non-secret key exchange parameters (1135, 1140) over an unsecured data channel and secure communications over a data channel.



Designated States: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW.
African Regional Intellectual Property Org. (ARIPO) (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW)
Eurasian Patent Organization (EAPO) (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM)
European Patent Office (EPO) (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR)
African Intellectual Property Organization (OAPI) (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publication Language: English (EN)